平成30年度　卒 業 論 文

和文題目

グループ鍵を利用した相手認証方式の提案

英文題目

Proposal for Node Authentication with Group Key

情報工学科　渡邊研究室

(学籍番号: 150441022)

右京　康也

提出日: 平成31年2月8日

名城大学理工学部

概要

企業ネットワークにおいて、業務ごとに通信グループを構築することは、セキュリティを高める上で有効な手段である。IPsec を用いれば前述のような通信グループを構築することができる。しかし IPsec を利用するには端末ごとに多くの項目を設定する必要があり、実用性が低い。

そこで、事前に共有されたグループ鍵と乱数のハッシュ値を通信開始時に交換することにより、相手認証を行う通信方式を提案する。送信側はグループ鍵と乱数から計算したハッシュ値と乱数を送信する。受信側は受け取った乱数と自分が持つグループ鍵からハッシュ値を計算し、送られてきたハッシュ値と比較することで相手を認証することができる。これによりより簡易にセキュアな通信グループを構築することができる。グループ鍵の共有方法は手入力またはグループ管理サーバ GMS（Group Management Server）からの配送で行う。

本論文では、提案の一部を実装し、提案方式の一部を実装し、仮想環境において動作検証と計測を行った。その結果から実用上問題がない時間で処理を行うことができることを確認した。

目 次

第 1 章　はじめに **1**

第 2 章　既存技術 **3**

2.1　グルーピングの具体例 3

2.2　IPsec の概要 4

2.3　IPsec を用いたグルーピング 4

2.4　同一のグループ鍵を用いたグルーピング手法 5

第 3 章　NTMobile **6**

3.1　概要 6

3.2　NTMobile のシーケンス 7

第 4 章　提案方式 **8**

4.1　提案方式の概要 8

4.2　提案方式における相手認証の流れ 8

4.3　提案方式のシーケンス 9

第 5 章　実装と評価 **11**

5.1　実装 11

5.2　動作検証 11

5.3　評価 12

5.3.1　処理時間の測定 12

5.3.2　結果 12

第 6 章　まとめ **14**

謝辞 **15**

参考文献 **17**

研究業績 **19**

第1章　はじめに

企業ネットワークにおけるセキュリティ脅威は、インターネット側だけでなく、イントラネット内部にも存在する。例えば、2014 年に自動車企業の元社員が、本社のサーバから機密情報を持ち出し、転職先の企業へ提供したとして、逮捕された。この事件のほかにも社員による情報漏洩は多数起こっている。こうした事件が背景となり、企業ネットワークには、業務ごとにセキュアな通信グループを構築したいという要求が存在する。IPsec を用いれば前述のような通信グループを構築することができる。IPsec は IETF(Internet Engineering Task) において、IP(Internet Protocol) レベルの暗号化機能として RFC6071 標準化されている。IPsec では、IP に対して様々なセキュリティを付加することができ、トンネリング、相手認証、暗号化などが可能である。IPsec は、主に拠点間をセキュアに接続するための VPN(Virtual Private Network) を構築するために用いられる。しかし通信する全ての端末間で、設定を行えば、実質的にセキュアな通信グループの構築が可能になる。しかし、この方法で通信グループを構築すると、大規模なシステムでは管理負荷が莫大になり、実用性が低い。

そこで、グルーピングを行う全ての端末に同一の鍵を共有する手法が注目されている。渡邊研究室では、この手法に用いる鍵を安全に配送する研究を行っている。また渡邊研究室では NTMobile（Network Traversal with Mobility) というオリジナル技術を研究している。NTMobile ではパケットの暗号化および、パケットの認証は行っているが、エンドエンドでの相手認証がなかった。そこで、本稿ではグループ鍵は安全に共有されているという前提のもと、NTMobile に相手認証機能を追加した。送信側はグループ鍵と乱数から計算したハッシュ値と乱数を送信する。受信側は受け取った乱数と自分が持つグループ鍵からハッシュ値を計算し、送られてきたハッシュ値と比較することで相手を認証することができる。これにより、より簡易にセキュアな通信グループを構築することができる。

グループ鍵の共有方法は、グループ管理サーバ GMS（Group Management Server）からの配送、もしくはパスワードの手入力の 2 つから選択できるようにする。大規模なシステムであれば前者を、小規模なシステムであれば、後者を用いる。前述の 2 つの方式でグループ鍵を共有できるようにするため、グループ鍵を格納する所定のファイルを各端末に持たせる。GMS は NTMobile でグルーピングを実現するために別途研究しているグループ管理サーバである。GMS はグループ情報の管理とグループ鍵の生成、配送を行う。

本稿では、移動透過性と NAT 越え通信の両者を同時に実現する NTMobile を利用して提案方式の実装を行った。実装では、グループ鍵の共有を手入力で行った。

以後、2 章では IPsec について説明する。3 章では NTMobile について説明し、4 章では提案方式の概要とシーケンスについて示す。5 章では提案方式の動作検証、処理時間の測定および既存技

術との比較を行い、最後に 6 章でまとめる。

第2章　既存技術

本章では、グルーピングの具体例とそれを実現する既存技術として、IPsec (Security Architecture for the Internet Protocol) の概要と課題について述べる。

2.1　グルーピングの具体例

図 1 にグルーピングの例を示す。図 1 は企業ネットワークの例であり、業務ごとにグループを構築している。人事サーバには人事部の社員のみがアクセスすることができ、極秘プロジェクトサーバにはプロジェクトメンバーのみがアクセスすることができる。また一般サーバには、全ての社員がアクセスすることができる。このようなグルーピングを可能にする技術として IPsec がある。

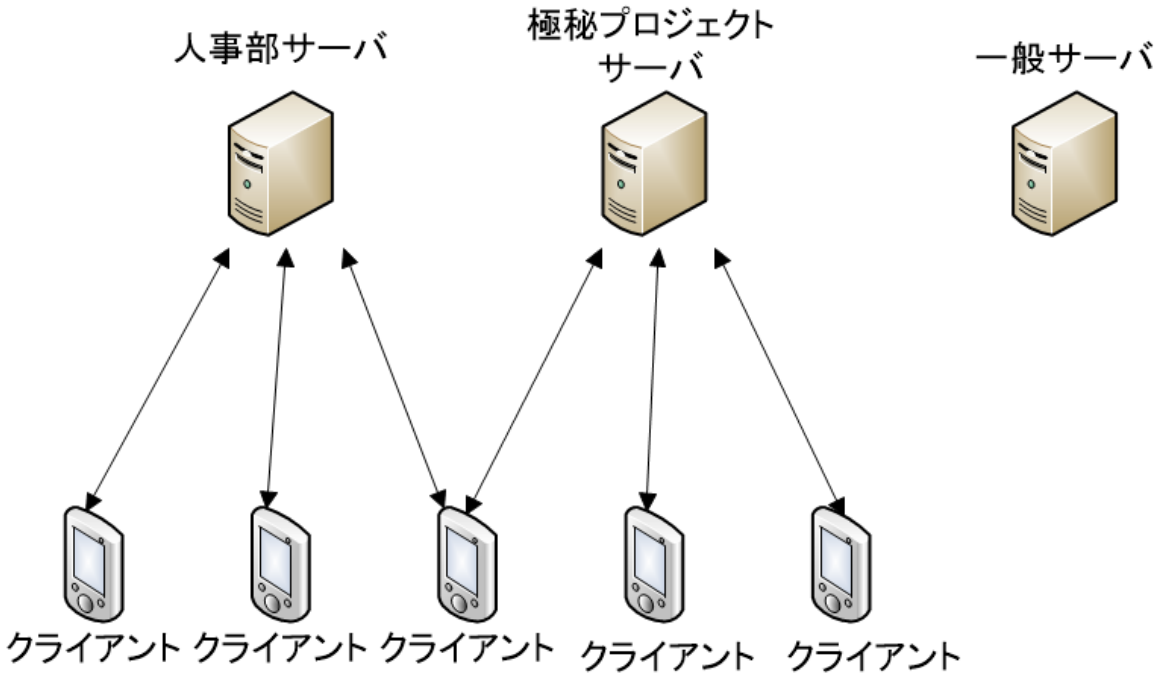

図 1　グルーピングの図

2.2 IPsecの概要

セキュアな通信グループを構築する通信方式としてIPsecを用いたグルーピングが考えられる。IPsecとはネットワーク層においてデータのセキュリティを保護するために使用されるプロトコルである。IPsecではIPに対して様々なセキュリティを付加することができ、トンネリング、相手認証、暗号化などが可能である。また通信は1対1であり、使用するにあたり必要な設定項目が多くある。IPsecは主にVPN(Virtual Private Network)を構築するための技術として用いられる。図 2にその図を示す。

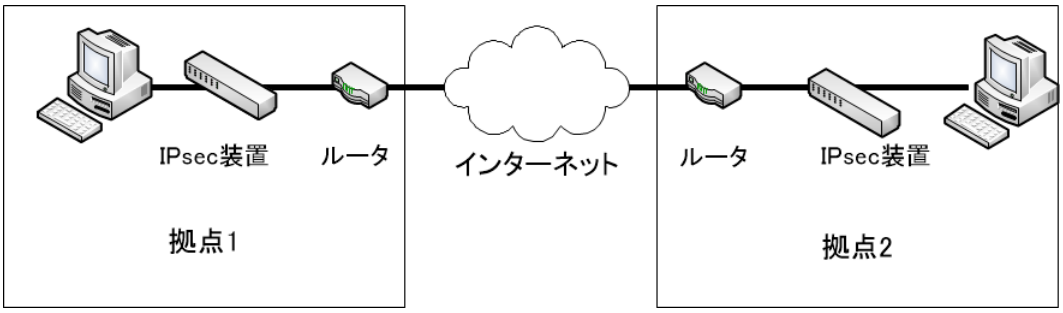

図 2　IPsecを用いたVPN

2.3 IPsecを用いたグルーピング

図 3にIPsecを用いたグルーピングを示す。全ての端末間で設定を行い、認証と暗号化を行うことによりセキュアな通信グループを構築することができる。しかし端末ごとに設定を行うことは実用上困難である。またIPsecは、セキュリティレベルが非常に高く、パケットの完全性の保証の対象にIPヘッダが含まれる。これによって、NATを経由することでアドレス情報が書き換えられると、不正パケットとして認証エラーが発生する。また暗号化の対象にTCP/UDPヘッダを含む場合があり、NAPTがポート番号の変更を行うことができない。このことからIPsecはNAT/NAPTを経由する通信では利用できず、システム構成が限定される。

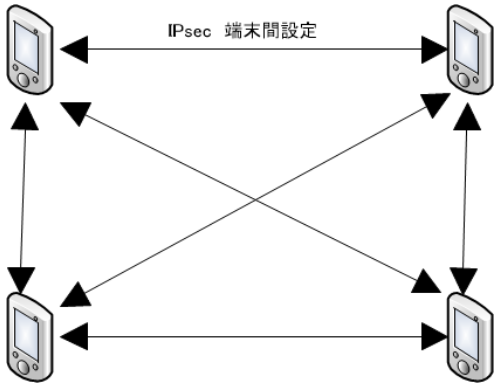

図 3　IPsecを用いたグルーピング

2.4　同一のグループ鍵を用いたグルーピング手法

IPsec では全ての端末間で個別に鍵を共有し、グルーピングを行っていた。しかし、この方法は管理負荷が大きく実用性が低い。よって図 4 のようなグループの全ての端末で同一の鍵を共有する手法が注目されている。また渡邊研究室では、このグルーピングに利用するグループ鍵を安全に配送するための技術として、GMS(Group Management Server) を研究している。GMS ではグループの作成、管理、グループ鍵の配送を行う。

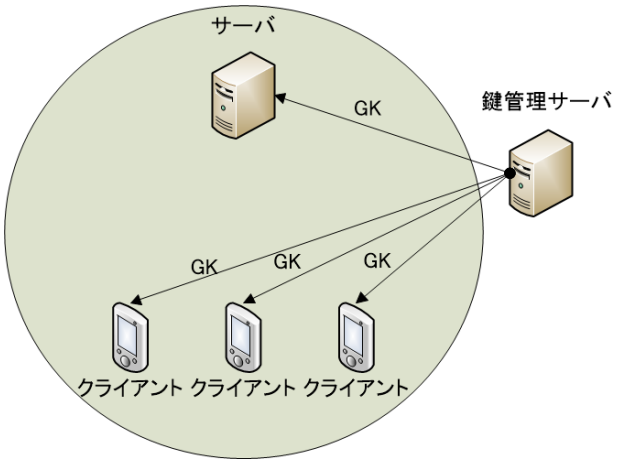

図 4　同一のグループ鍵を用いたグルーピング

第3章　NTMobile

本稿では、提案方式を NTMobile(Network Traversal with Mobility) を利用して実装する。そのため本章では移動透過性と NAT 越え通信の両者を同時に実現する NTMobile について、概要およびシーケンスについて説明する。

3.1　概要

NTMobile は、通信中にネットワークが切り替わっても通信を継続することができる移動透過性と、NAT の外側から通信を開始することができる NAT 越えの両者を同時に実現する技術である。NTMobile 端末は、通信開始時に DC(Direction Coordinator) からの経路指示によってトンネルを生成し、以後すべての通信で仮想アドレスのパケットを実アドレスでカプセル化する。図 5 に NTMobile の構成を示す。NTMobile は NTMobile 機能を実装したエンド端末（以後 NTM 端末）、NTM 端末のアドレス情報の管理、および通信経路の指示を行う DC、 エンドエンドで直接通信ができない場合にパケットの中継を行う RS（Relay Server）から構成される

通信を行う NTM 端末はシグナリングの過程において安全に End Key を共有する。この共通鍵を用いてエンドツーエンドでパケットの暗号化と、パケット認証を行う。しかし、相手認証機能は実装されていなかった。

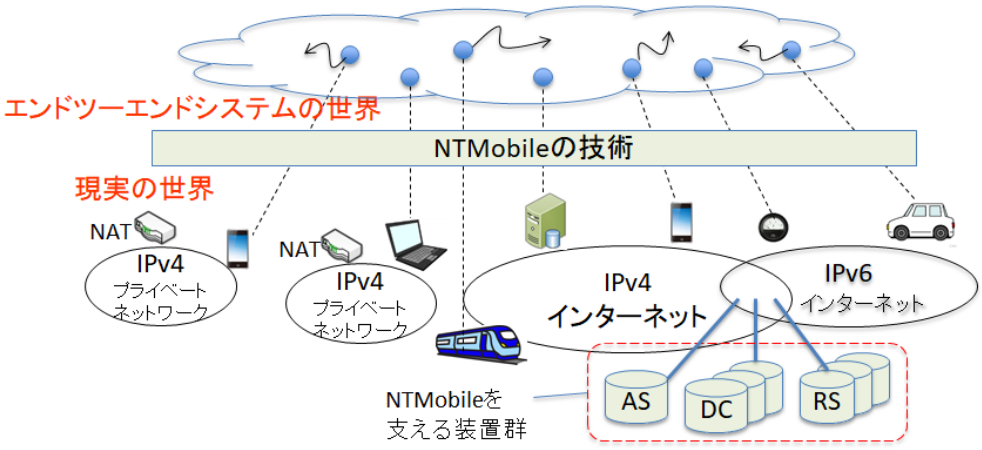

図 5　NTMobile の構成図

3.2 NTMobile のシーケンス

図 6 に NTMobile のシーケンスを示す。なおこのシーケンスは NTMobile のシーケンスを説明するための最も簡易なものであり、NAT は省略している。また MN、CN はそれぞれ安全に、DC と共通鍵を共有している。この共通鍵を利用して Direction Request、Route Direction のパケットを暗号化している。MN(Mobile Node) の FQDNcn の名前解決処理をトリガーとして、DC(Direction Coordinator) に Direction Request が送信される。Direction Request を受け取った DC は、MN と CN(Correspondent Node) に対して Route Direciton で経路を指示する。経路指示を受け取った MN と CN は DC の指示に従って Tunnel Request/Tunnel Respose を交換し、End Key の共有と通信経路の確立を行う。また Tunnel Request は Route Direction の際に受け取る Temp Key で暗号化され、Tunnel Respose は End Key によって暗号化されている。共有した End Key はエンドツーエンドのパケット暗号化およびパケット認証に用いられる。

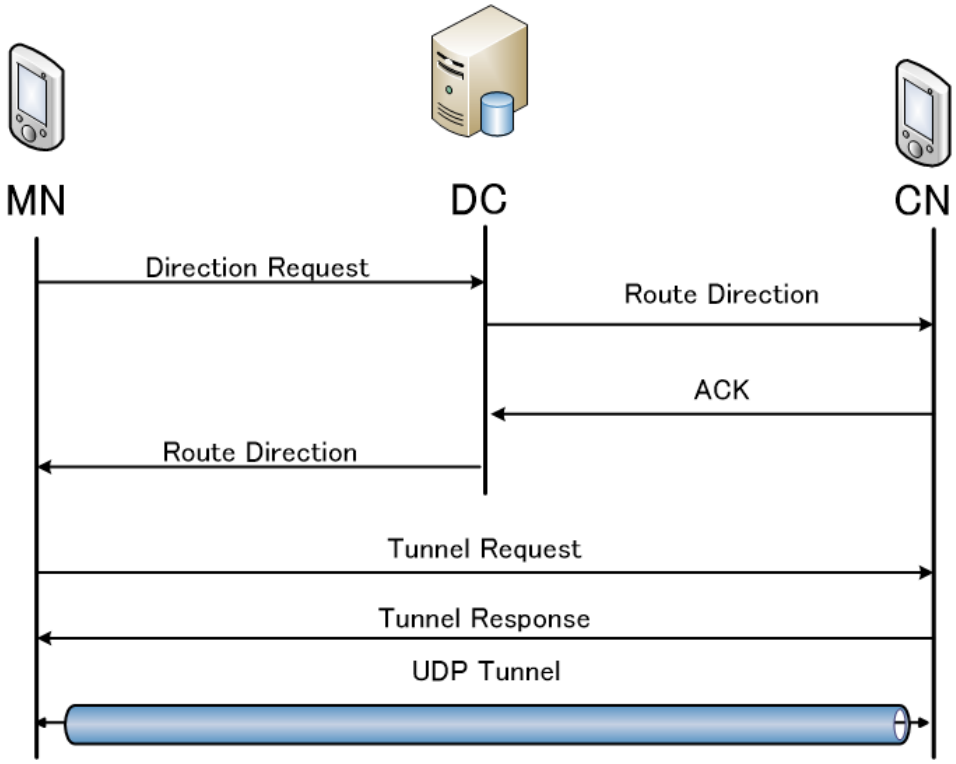

図 6　NTMobile のシーケンス

第4章　提案方式

本章では、提案する相手認証方式の概要、提案方式における相手認証の方法および相手認証機能を加えた NTMobile のシーケンスについて説明する。

4.1　提案方式の概要

提案方式は、企業ネットワークにおいて用いられることを想定している。例を図 7 に示す。グルーピングをしたサーバごとに業務をわけることによって、業務に関与する権限のないクライアントからのアクセスを拒否することができる。またクライアントは自分の所属しているグループ名を把握しており、鍵を複数所持する場合は、クライアントが使用する鍵を選択することを想定している。同様にグループ鍵を所持していないサーバに対しては、鍵を指定しないことで通信を可能にする。このように提案方式を用いれば業務ごとに通信グループを構築することができ、セキュリティを高めることができる。

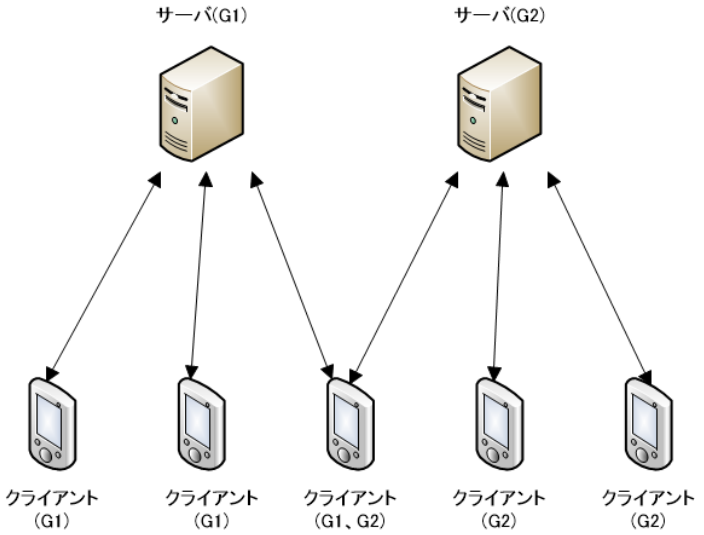

図 7　提案方式の利用例

4.2　提案方式における相手認証の流れ

図 8 に提案方式における相手認証の方法を示す。図 8 では CN が MN を認証する処理を示している。OTC(one time code) は使い捨てで十分大きな乱数であり、GK はグループ鍵、h（GK||OTC）

はGKとOTCのハッシュ値である。MN、CNは同一グループのメンバであり、GKを事前に共有している。MNは自分で生成した乱数OTC1と所持している鍵GKから、ハッシュ値を生成する。生成したハッシュ値h（GK||OTC1）とOTC1をCNに送信する。CNは受信したOTC1と所持しているGKからハッシュ値を計算する。計算したハッシュ値と受信したハッシュ値を比較し、一致すればMNを認証することができる。同様の処理をCN側から行い、ハッシュ値が一致すれば相互認証が完了する。

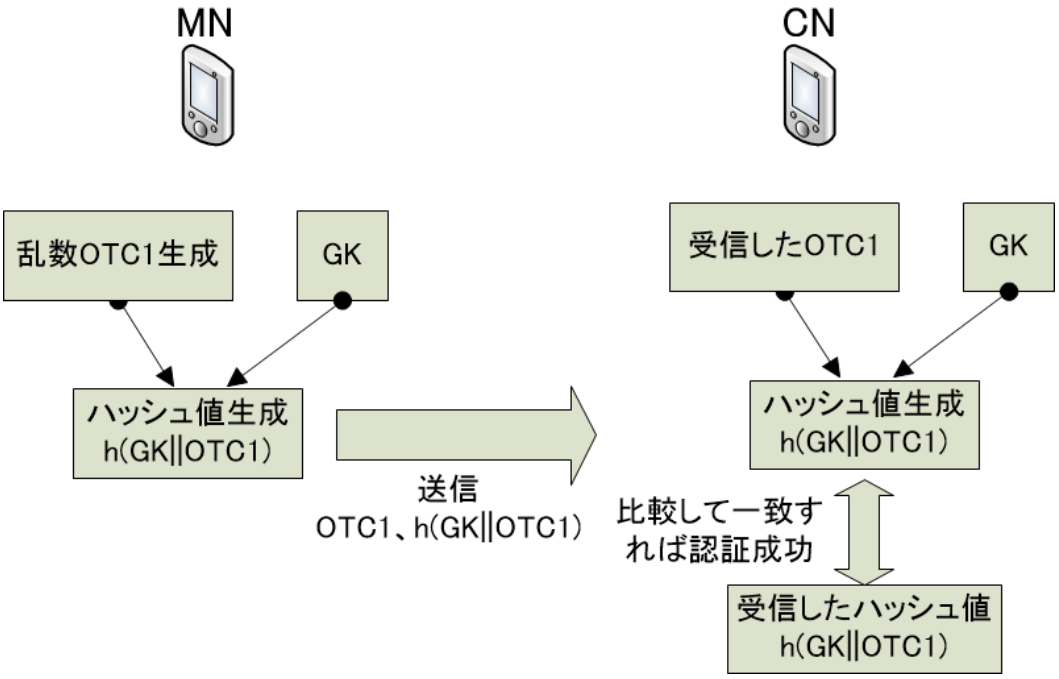

図 8　提案方式における相手認証の方法

4.3　提案方式のシーケンス

図 9に提案方式のシーケンスを示す。4.2で述べた処理を従来のNTMobileのシーケンスに組み込んだ。NTMobileの通信開始時のシーケンスにおいて、Tunnel Request/Responseで初めてエンドエンドで通信を行う。よってTunnel Request/Tunnel Resposeにh（GK||OTC）とOTCを追加した。図 10に提案方式におけるTunnel Requestのヘッダフォーマットを示す。NTM HeaderはNTMobile特有のヘッダー、TempKey(End Key）はEnd KeyをDCから配布されたTempKeyで暗号化したもの、HMACは認証コードである。ただしHMACはパケットの認証を行う認証コードであり、相手認証を行うものではない。ここに今回h（GK||OTC1）とOTC1を追加した。Tunnel ResposeもTunnel Requestと同様の変更を加えた。

グループ鍵の共有方法は、グループ管理サーバGMS（Group Management Server）からの配送、もしくはパスワードの手入力の2つから選択できるようにする。大規模なシステムであれば前者を、小規模なシステムであれば、後者を用いる。前述の2つの方式でグループ鍵を共有できるよ

うにするため、グループ鍵を格納する所定のファイルを各端末に持たせる。

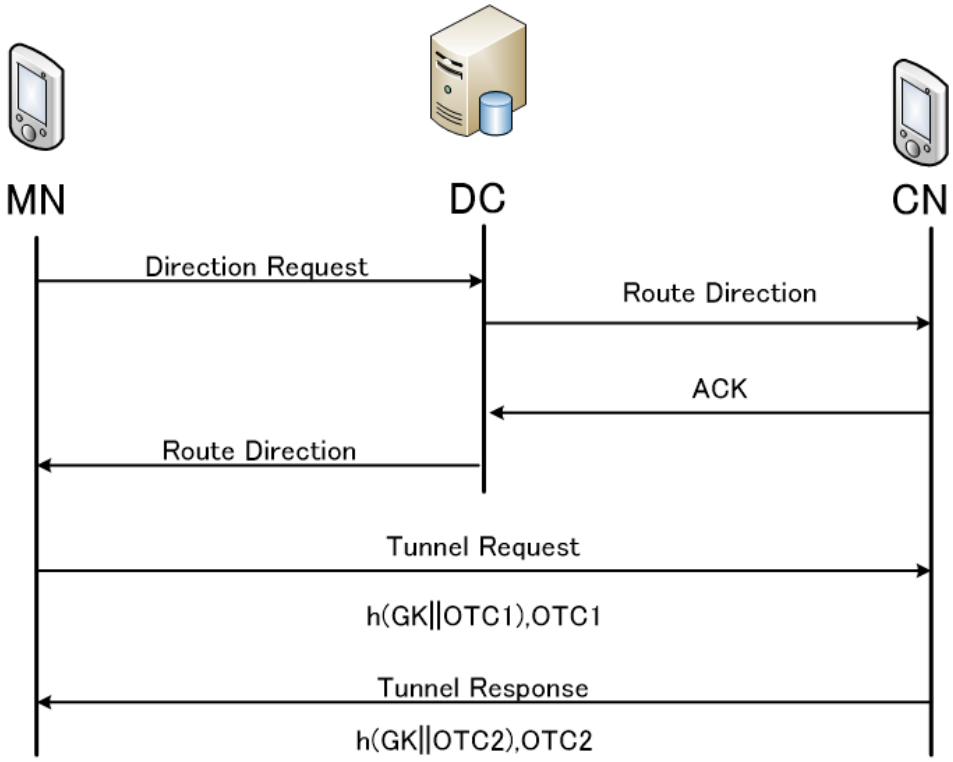

図 **9**　提案方式のシーケンス

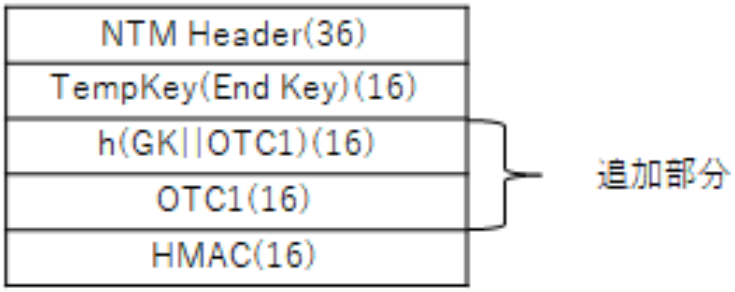

図 **10**　**Tunnel Request** のパケットフォーマット

第5章　実装と評価

本章では、提案方式の実装および動作検証について述べる。実装は Linux 環境で行った。

5.1　実装

実装では、グループ鍵の共有を手入力で行った。Tunnel Request/Response 生成処理に、乱数の生成および、ハッシュ値の生成処理を加えた。Tunnel Request/Response 受信処理にハッシュ値検証処理を加えた。

5.2　動作検証

表 1 にホスト PC の仕様、表 2 に仮想環境の仕様を示す。1 台のホスト PC 上に VMware Player を用いて MN、CN の 2 台を構築した。また DC についてはローカルネットワーク上に構築されているものを利用した。図 11 に動作検証を行ったネットワーク構成を示す。提案方式において、MN、CN では乱数とハッシュ値の生成、およびハッシュ値の検証を行う。MN、CN において乱数とハッシュ値の生成、およびハッシュ値の検証が正しく行われていることを確認した。これにより NTMobile においてグループ鍵を利用した相手認証の実現ができた。

表 1　ホスト PC の構成

	ホスト PC
OS	Windows10 64bit
CPU	Intel Core i3-3220 3.30GHz
Memory	4.00GB

表 2　仮想環境の構成

	MN、CN
OS	Ubuntu 14.04
CPU	Intel Core i3-3220 3.30GHz
Memory	各 1.00GB

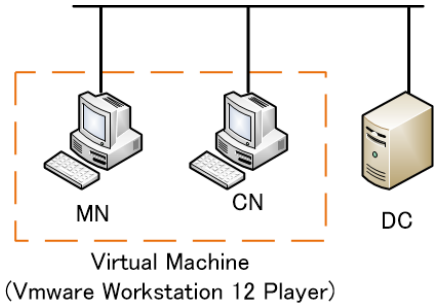

図 11　装置の構成

5.3　評価

提案方式の性能評価を実施した。

5.3.1　処理時間の測定

提案方式では、NTMobile シーケンスの Tunnel Request/Tunnel Respose パケットに情報を追加した。また MN と CN に、乱数、ハッシュ値の生成、およびハッシュ値の検証を行う処理を追加した。よって処理時間が変化するのは、MN が DC からの Route Direction を受信してから、CN と Tunnel Request/Tunnel Respose パケットの交換が終わり、次のパケットを送信するまでである。従来のシーケンスと比較し、処理時間が増加する箇所を、明記したシーケンスを図 12 に示す。この処理時間の測定を 10 回行いその平均時間を算出した。パケットの観測には Wireshark を利用した。

5.3.2　結果

表 3 に実行結果を示す。この表を見ると従来の方式から処理時間が 4.943×10^{-4} 秒増加していることが分かる。提案方式をシーケンスに組み込んだ結果、4.943×10^{-4} 秒処理時間が増加してしてしまったが、このシーケンスは通信開始時のみ行われるものである。よって提案方式の実装は、実用上問題ないと考えられる。

表 3　実行結果

	従来方式	提案方式
処理時間 (s)	2.735×10^{-1}	2.740×10^{-1}
増加時間 (s)	0	4.943×10^{-4}

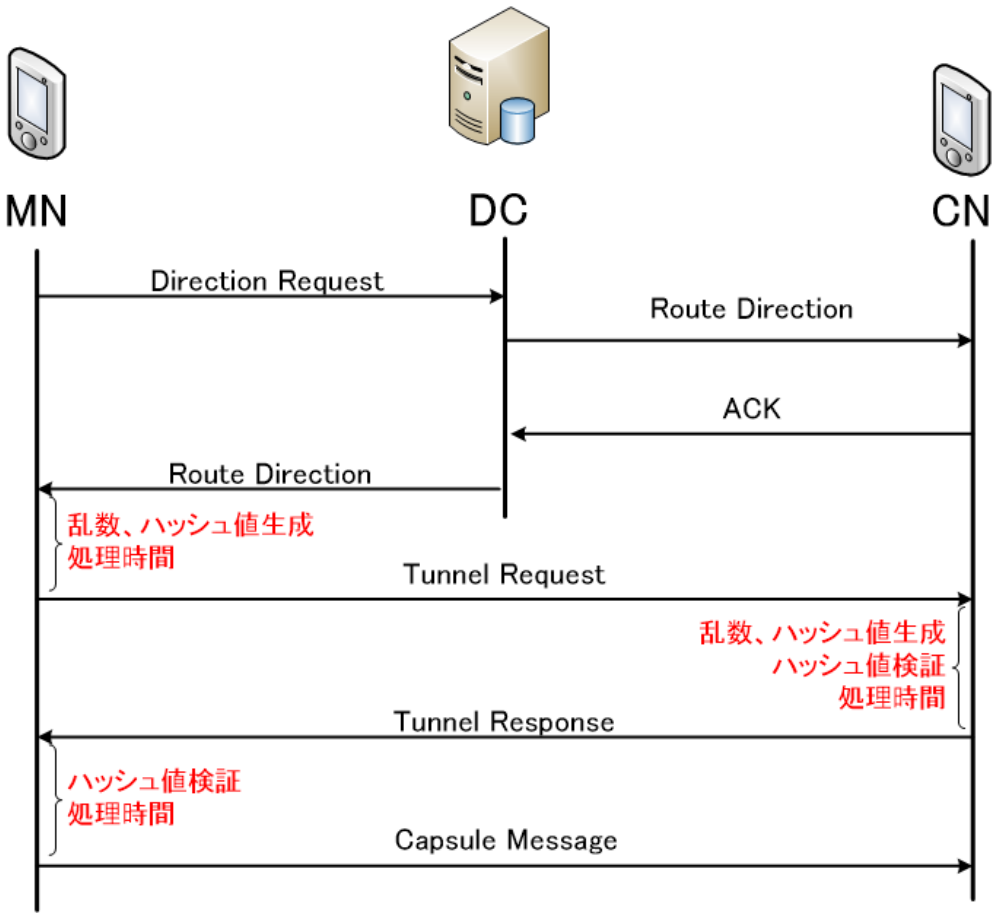

図 **12**　計測箇所を明示したシーケンス図

第6章　まとめ

本稿では、NTMobile を用いて、事前に共有されたグループ鍵を利用し、相手認証を行う通信方式の提案と実装を行った。NTMobile の Tunnel Request/Tunnel Respose においてグループ鍵と乱数のハッシュ値を交換、検証することにより、相手認証を可能にした。また Linux 上で提案方式の実装を行い、動作検証を行った。従来の方式と提案方式を比較し、処理時間は増加するものの実用上問題がないということを示した。

今回の実装ではグループ鍵の共有は手入力で行った。今後は、グループ鍵の共有方法に GMS を利用した場合の実装について進めていく予定である。

謝辞

本研究を進めるにあたり、多大なるご指導を賜りました、指導教官である名城大学理工学部情報工学科　渡邊晃教授に心から感謝致します。

本研究を進めるにあたり、様々なご指導を賜りました、名城大学理工学部情報工学科　鈴木秀和准教授に深謝致します。

本研究を進めるにあたり、様々なご助言を賜りました、愛知工業大学情報科学部情報科学科　内藤克浩准教授に拝謝致します。

本研究を進めるに当たり、常に迅速かつ適切なご意見並びに助言を賜りました、菅沼氏に心から感謝いたします。

最後に、本研究を進めるにあたり、日頃から多くの有益なご意見を賜りました、渡邊研究室の皆様、鈴木研究室の皆様、NTMobile の研究に携わる皆様に感謝致します。

参考文献

[1] 馬場達也：マスタリング IPsec，オライリー・ジャパン (2001).
[2] 小早川知昭：IPsec 徹底入門， 翔泳社 (2002).
[3] 渡邊　晃，厚井裕司，井手口哲夫，横山幸雄，妹尾尚一郎：IPv4/IPv6 暗号技術を用いたセキュア通信グループの構築方式とその実現，情報処理学会論文誌，Vol. 38, No. 4, pp. 904-914 (1997).
[4] 鈴木秀和，渡邊　晃：フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の実装と評価，情報処理学会論文誌，Vol. 47, No. 11, pp. 2976-2991 (2006).
[5] 上醉尾一真，鈴木秀和，内藤克浩，渡邊　晃：IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価，情報処理学会論文誌，Vol. 54, No. 10, pp. 2288-2299 (2013).
[6] 棚田慎也，鈴木秀和，内藤克浩，渡邊　晃：暗号技術を用いたセキュアグループコミュニケーションの提案，マルチメディア，分散，協調とモバイル（DICOMO2016）シンポジウム論文集，pp.366-371 (2016).
[7] 納堂博史，八里栄輔，鈴木秀和，内藤克浩，渡邊　晃：実用化に向けた NTMobile フレームワークの実装と評価，第 82 回 MBL・第 53 回 UBI 合同研究発表会，No. 46, pp. 1-8 (2017).

研究業績

研究会・大会等（査読なし）

（1）右京康也, 菅沼良一, 鈴木秀和, 内藤克浩, 渡邊晃：NTMobile におけるグループ鍵を利用した相手認証の提案，平成 30 年度電気・電子・情報関係学会東海支部連合大会論文集, No. L1-1, Sep. 2018.